Minimize Your New & Emerging Business Risks

When a major crisis strikes, the disruption it creates has immediate and lasting impacts on organizations’ workforces, security operations and business continuity programs. Here are three immediate and longer-term challenges that crisis events create and ways RSA can help you address them.

Challenge 1: Workforce Transformation

What happens when employees can’t commute to the office, travel for business or work on site? RSA SecurID Suite can help you quickly stand up a secure remote workforce.

Multi-Factor Authentication
RSA SecurID Access helps to ensure that all remote users accessing your VPN, cloud-based and on-premise systems are who they say they are.

Identity Governance & Lifecycle Management
RSA Identity Governance and Lifecycle streamlines your identity and access management processes. Control and monitor user access and entitlements, automate onboarding and deprovisioning, and ensure compliance.

Challenge 2: Security Transformation

How do you manage security operations when everyone is remote? Do your policies and procedures assume your critical response teams are all working from a single location? And are you prepared for the influx of phishing emails and other forms of fraud that cybercriminals are perpetrating to prey on remote workers and consumers?

Remote SOC
RSA NetWitness Platform provides security teams with visibility across endpoints, the network and the cloud. When your security team is geographically dispersed, you need a single, unified platform, not multiple disparate tools.

Threat Management Service
RSA FraudAction is a single, external threat management service that provides 24x7 detection and mitigation of online threats including phishing, Trojans, rogue mobile apps and rogue social media pages.

Challenge 3: Business Continuity

What do you do when the harsh realities of a crisis upend your existing business continuity and recovery plans?

Business Resiliency
RSA Archer Business Resiliency offers an automated approach to resiliency planning and recovery, allowing your organization to be prepared and respond quickly in crisis situations to sustain daily business operations.

Third-Party Risk
RSA Archer Third Party Governance enables your organization to efficiently manage third-party ecosystem to understand and act on the related risks in an integrated manner. RSA brings together the intelligence, capabilities and business context to help you optimally manage your third parties.

CONSIDERATIONS FOR SECURITY & RISK

- Physical site impacts
- Mobile controls
- Secure remote access

CONSIDERATIONS FOR SECURITY & RISK

- Expanded attack surface
- Network & endpoint visibility
- Network detection
- Network resiliency

CONSIDERATIONS FOR SECURITY & RISK

- Addressable data
- Audit third-party
- Audit third-party
- Compliance audits

RSA believes the information in this document is accurate. The information is subject to change without notice. ©2020 RSA Security LLC or its affiliates. All rights reserved. RSA and the RSA logo are registered trademarks or trademarks of RSA Security LLC or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners.